

4/PRTS

10/519733
DT01 Rec'd PCT/PTC 28 DEC 2004

Attorney Docket 004708-105838

SPECIFICATION

5

TITLE OF THE INVENTION

Product Authentication System for Preventing Distribution of
Counterfeits in Market

10 TECHNICAL FIELD OF THE INVENTION

The present invention relates to a product authentication system
for providing in an ASP system product authentication service at
a distribution stage for the purpose of protecting, by means of
preventing counterfeits on the market from entering the distribution
15 channel, the benefit of manufacturers, dealers, distributors, and
consumers forming the distribution channel.

DESCRIPTION OF THE RELATED ART

When consumers purchase a product which adorns themselves such
20 as a wrist watch, a bag, or clothing, who manufactured the product
is an important decisive factor in selecting the product. The value
such a product which adorns consumers should have is not only that
the product satisfies a required function but also that the product
is excellent as a means for self-actualization. A brand is value
25 added to a product in that it can directly represent particularities

of a person who buys the product. Therefore, a manufacturer having a strong brand applies an original unified design on its products or intentionally provides a registered trademark or a logo at a conspicuous location of its products, so that it is made clear at
5 a glance that the product is manufactured by the manufacturer. A consumer who buys the product can show off the brand of the manufacturer to represent his/her particularities just by carrying the product with him/her. In the context of such a trend in consumption, manufacturers, for the purpose of increasing their
10 market shares, have put efforts into enhancing their brand power to increase the added value of their products.

However, on the other hand, by taking advantage of such a trend in consumption, counterfeits manufactured so as to be just like high-value-added brands are sometimes on the market and sold at lower
15 prices and in high volume. As the copying technology of counterfeits becomes sophisticated and their distribution channel is shrewdly formed evading control, counterfeits take market share away from genuine products in the market of brands. Manufacturers of such products suffer from heavy economic losses, because, not only the
20 sales of their products are hurt, but also, for example, troubles caused by counterfeits damage the credibility of the brand and considerably degrade the value of the brand.

Further, dealers and distributors who can not tell counterfeits deal with counterfeits, thinking that the counterfeits are genuine
25 products. Detection that the products dealt with by such dealers

and distributors are counterfeits leads to a large amount of dead stock. When they have already sold such counterfeits, they have to recall the counterfeits from those who have purchased the counterfeits, change the counterfeits for genuine products, or the
5 like, as a guarantee for the purchaser. In this way, such dealers and distributors suffer from heavy economic losses.

Further, consumers who can not tell counterfeits and who have purchased counterfeits thinking that they are genuine products also suffer from economic losses when they purchase the counterfeits
10 abroad during their travel and the like. Even if what they have purchased is revealed to be counterfeits after the purchase, it is difficult to negotiate about returning the counterfeits. When troubles such as breakdown are caused after they return home, they can not make what they have purchased returned or changed for genuine
15 products, because they do not know how to contact the dealers, the necessary procedure is complicated, or the like.

As described in the above, counterfeits inflict losses on everyone who forms a distribution channel, i.e., from manufacturers, through dealers and distributors, and to consumers.

20 Therefore, manufacturers take the following measures in order to discriminate between their own products and counterfeits.

Sometimes products are highly elaborated by the manufacturers as a means for characterizing the products as genuine products. More specifically, the material is embossed, the design is provided with
25 a complicated pattern of shape or color, the products are of elaborate

craftsmanship by skilled manual work, a registered trademark or a logo is placed on a specific location, or the like. These not only have the effect of enhancing the added value in design, but also have the effect of preventing counterfeiting by making it technically
5 difficult to imitate their products.

In such a case, whether the product is a genuine one or an counterfeit is discriminated in the following way: when a characterized portion of the product sufficiently looks like that of a genuine product, it is determined to be a genuine product; when
10 the characterized portion of the product does not sufficiently look like that of a genuine product, it is determined to be an counterfeit.

Further, in some cases, manufacturers issue guarantees or warranty cards for guaranteeing their products and attach them on their products. Such guarantees or the like have their respective
15 serial numbers described or inscribed thereon, or, are of elaborate craftsmanship with stamps or watermarks which are technically difficult to imitate.

In such a case, whether the product is a genuine one or an counterfeit is discriminated in the following way: when the product
20 has a guarantee or the like attached thereto and the guarantee or the like sufficiently looks like a genuine guarantee or the like, it is determined to be a genuine product; when the guarantee or the like does not sufficiently look like a genuine guarantee or the like, it is determined to be an counterfeit.

25 Further, in some cases, manufacturers seal packages of their

products with hologram seals or the like which are technically difficult to imitate such that the packages are not easily opened.

In such a case, whether the product is a genuine one or an counterfeit is discriminated in the following way: when there is
5 no trace that a seal for sealing the package of the product was opened, it is determined to be a genuine product; when there is a trace that the seal was opened, it is determined to be an counterfeit.

SUMMARY OF THE INVENTION

10 When it is discriminated whether a product is a genuine one or an counterfeit by the conventional methods described in the above and a genuine product is authenticated, there are the following problems.

First, as for representation of elaborate craftsmanship in
15 design, a registered trademark, or the like, if the accuracy of counterfeits is enhanced, the counterfeits can sufficiently look like a genuine product. Therefore, such discrimination requires expertise for discriminating subtle differences, and discriminators have to be trained or employed. But still, if a genuine product
20 and a counterfeit can not be identified, no discrimination can be made.

Further, as for a guarantee attached to a product, similarly, if the accuracy of counterfeits is enhanced, a counterfeit guarantee can sufficiently look like a genuine guarantee. Therefore, if a
25 counterfeit guarantee attached to a counterfeit and a genuine

guarantee attached to a genuine product can not be identified, no discrimination can be made between a genuine product and a counterfeit. Further, when a guarantee is of elaborate craftsmanship with a stamp or a watermark, expertise for discriminating differences is newly
5 required. Insufficient expertise may be counterproductive, since even a counterfeit which looks like genuine under casual inspection can be easily believed to be genuine.

Further, when a package of a product is sealed with a seal of elaborate craftsmanship, for example, a hologram seal, a purchaser
10 can not open the package prior to purchase and can not examine the content therein, which causes a demerit of leading to decrease in purchasing motivation. Further, manufacture of such seals incurs additional cost. Still further, when such a seal is of elaborate craftsmanship, for example, when such a seal is a hologram seal,
15 expertise for discrimination is newly required as in the case of a guarantee described in the above. With insufficient expertise, even a counterfeit seal which looks like a genuine seal under casual inspection can not be discriminated.

As described in the above, the conventional methods of
20 discriminating differences in the outer appearance by means of manual inspection of a product itself, its guarantee, a seal for sealing its package, or the like require expertise for the discrimination as well as time necessary for the discrimination. Therefore, at a distribution stage, accurate discrimination of a large amount of
25 products at a low cost, without difficulty, at an arbitrary place,

and in a short time can not be made.

In view of the above-described conventional problems involved in discrimination between genuine products and counterfeits in a product distribution market, an object of the present invention is
5 to provide a criterion for discrimination between genuine products and counterfeits other than differences in the outer appearance, and, further, to make a discriminating method capable of being performed not as manual work but as a mechanical process and to make available convenient discrimination between genuine products and
10 counterfeits via the Internet for distributors and dealers who deal with products.

According to the present invention, to attain the object as described in the above, a product authentication system is established, wherein a non-contact tag, a reader, a database, a data
15 server, and an authentication server are prepared as hardware for forming the product authentication system.

The non-contact tag is embedded as an authentication device in a product to be authenticated. The non-contact tag has a specific ID known only to an administrator of the product authentication system,
20 the ID being stored in a body of the non-contact tag as electronic data.

The reader reads ID data of the non-contact tag. The reader has a specific ID known only to the administrator of the product authentication system, the ID being stored in a body of the reader
25 as electronic data, and the reader has means for connecting to the

Internet for communication.

The database stores the ID data and attribute information data of the non-contact tag, product information data of the product having the non-contact tag embedded therein, and the ID data and attribute
5 information data of the reader, and has means for connecting to the Internet for communication.

The data server reads data stored in the database and writes data into the database, and has means for connecting to the Internet for communication.

10 The authentication server checks the ID data of the reader and the ID data of the non-contact tag sent from the reader connected to the Internet against data stored in the database to authenticate the reader and the non-contact tag, and has means for connecting to the Internet for communication.

15 Using such hardware, whether a product is a genuine one or not is discriminated in the following steps.

First, prior to distribution of the non-contact tag and the reader to a user of the product authentication system, the data server reads the ID data of the non-contact tag and the ID data of the reader,
20 creates data files thereof, and stores the data files in the database.

Subsequent to the distribution of the non-contact tag and the reader to the user of the product authentication system, the reader connected to the Internet reads its own ID data and sends it to the authentication server. The authentication server checks the
25 received ID data of the reader against the data file of the reader

stored in the database.

The authentication server notifies the reader checked against the identical ID data that the reader is authenticated, and urges the reader to send the ID data of the non-contact tag embedded in
5 the product.

The authenticated reader reads the ID data of the non-contact tag embedded in the product and sends the ID data to the authentication server. The authentication server checks the received ID data of the non-contact tag against the data file of the non-contact tag
10 stored in the database.

The authentication server notifies the reader which sent the ID data of the non-contact tag that the non-contact tag checked against the identical ID data is authenticated.

Further, the above-described product authentication system may
15 be administered and operated by an application service provider (ASP) entity to provide product authentication service via the Internet in an ASP system.

Further, in the above-described product authentication system, when the side of the user is made to have a double ID by assigning
20 to the user of the reader a specific password known only to the administrator and the user of the reader, by adding the following steps, the product authentication system can be made to have a triple checking function as a whole.

The data server creates a data file of data of the assigned
25 password as attribute information related to the ID data of the

distributed reader, and stores the data file in the database.

After the reader is notified of its authentication, the authentication server requests input of the password of the user, receives password data inputted and sent from a terminal of the user,
5 and checks said password data against the data file stored in the database.

When check against the identical password data is made, the authentication server notifies the user terminal which sent the password data that the password is authenticated.

10 Further, the following steps can be added to the above-described product authentication system.

The reader and the user terminal distributed to the manufacturer of the product who is the user of the product authentication system sends to the data server product information data such as the name,
15 the model, the date of manufacture, and the place of manufacture of the product, the product information data being related to the ID data of the non-contact tag.

The data server receives the product information and creates a data file as attribute information related to the ID data of the
20 embedded non-contact tag, and stores the data file in the database.

By adding the above-described steps, when, for example, someone attempts to obtain authentication and to sell a counterfeit by taking off a non-contact tag embedded in an inexpensive genuine product and attaching the non-contact tag to a counterfeit of a more expensive
25 genuine product, such abuse can be prevented by referring to the

product information such as the name and the model of the product in addition to the ID of the non-contact tag.

Further, the following steps can be added to the above-described product authentication system.

5 A manufacturer of the non-contact tag creates a data file where the ID of the non-contact tag is related to the manufacturer of the product who is a supplier of the non-contact tag, and sends the data file to the data server.

10 The data server receives the data file and stores the data file in the database.

The authentication server receives the ID data of the non-contact tag sent from the reader, and checks whether the ID is related to the supplier in the data file of the non-contact tag stored in the database.

15 By the above steps, authentication of a product becomes two-step. More specifically, first, whether the ID of the non-contact tag is related to the supplier is checked, and then, whether the ID of the non-contact tag is related to the product information is checked, and thus, a counterfeit can be detected more efficiently, and at
20 the same time, the reliability can be increased.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a view describing an overview of an embodiment of a product authentication system according to the present invention,
25 and illustrating roles of parties concerned in the system by showing

flow of materials and flow of information.

Fig. 2 is a view describing a configuration of hardware necessary for implementing the embodiment of the product authentication system, and showing hardware to be provided for each party concerned.

5 Fig. 3 is a view describing in detail information processing for implementing the embodiment of the product authentication system with the hardware shown in Fig. 2, and showing contents and directions of information exchanged between pieces of the hardware.

Fig. 4 is a view describing response of the product
10 authentication system when an attempt is made to use the product authentication system without proper authorization compared with a case where the system is used with authorization.

DETAILED DESCRIPTION OF THE INVENTION

15 Next, with reference to the drawings, an embodiment of the present invention is described specifically and in detail.

First, an overview of an embodiment of a product authentication system according to the present invention is described with reference to Fig. 1.

20 Parties concerned in a product authentication system are an ASP entity 10 who is an administrator, and, a manufacturer 20, a dealer 30, a distributor 40, and a consumer 50 who are users. The ASP entity 10 administers a non-contact tag 11 and a reader 12 to administer and operate the product authentication system and provides
25 product authentication service.

The ASP entity 10 supplies the manufacturer 20 with the non-contact tag 11. The non-contact tag 11 has a specific ID, and the ID is stored in a body of the non-contact tag as electronic data. The ASP entity 10 administers ID data of the non-contact tag 11, and data of attribute information such as the name of the manufacturer who is an supplier.

As for the above-described supply of the non-contact tag 11, a manufacturer of the non-contact tag 11 may directly supply the manufacturer 20 with the non-contact tag 11. In this case, the manufacturer of the non-contact tag 11 may create a data file where the ID of the non-contact tag 11 is related to the manufacturer 20 who is the supplier and may provide the data for the ASP entity 10.

As the non-contact tag 11, a super-micro IC chip with a communication function may be used. Such a super-micro IC chip includes one manufactured by Hitachi under the trade name of " μ chip". The chip measures 0.4 mm both in length and in width, and about 170 μ m in thickness, and thus, looks like only a small dot when put on a fingertip. With this size, the chip has a 128-bit memory and a function of communicating by radio waves of 2.45 GHz.

As is known to those skilled in the art, the non-contact tag 11 may be named in different ways, including wireless IC tag, next generation bar code, new generation bar code, ubiquitous ID, wireless IC chip, wireless ID tag, IC tag, non-contact IC tag, IC label, IT tag, non-contact IC card, auto ID, electronic tag, non-contact IC

tag, wireless tag, RFID tag, smart tag, non-contact IC chip, etc.

The ASP entity 10 leases to each user of the product authentication service the reader 12 for reading an IC code of the non-contact tag 11. The reader 12 can connect to the Internet via
5 a general-purpose terminal such as a personal computer, and has a specific ID. The ID is stored in a body of the reader as electronic data. The ASP entity 10 administers ID data of the reader 12, and data of attribute information such as the name of the user to whom the reader is leased.

10 In leasing the reader 12, the ASP entity 10 may make the side of the users have a double ID by assigning a specific password to each user. The ASP entity 10 administers data of the assigned password as attribute information data of the reader 12.

The manufacturer 20 embeds in a product the non-contact tag
15 11 supplied from the ASP entity 10. By embedding the non-contact tag inside the product so as not to be perceived from the outer appearance, the non-contact tag can be prevented from impairing the appearance of the product and from being taken off and abused. The manufacturer 20 connects its leased reader 12 to the Internet. After
20 the reader 12 is authenticated, the manufacturer 20 registers with the ASP entity 10 product information related to the non-contact tag 11 such as the name, the date of manufacture, and the place of manufacture of the product. The ASP entity 10 administers, in addition to the ID of the non-contact tag 11 and the name of the
25 manufacturer who is the supplier, the product information data

registered from the manufacturer 20, the product information data being related to the ID of the non-contact tag 11 and the name of the manufacturer.

After the reader 12 is authenticated, the manufacturer 20 can
5 browse the registered data.

The dealer 30 and the distributor 40 connect their respective leased readers 12 to the Internet. After their respective readers 12 are authenticated, the dealer 30 and the distributor 40 inquire the ASP entity 10 whether a product they deal with is authenticated
10 to be a genuine product. The ASP entity 10 checks the ID data of the inquired non-contact tag 11 against its administered data, authenticates the product, and notifies the dealer 30 and the distributor 40 of the result.

At the time of purchase of the product, the consumer 50 can
15 request the dealer 30 to show evidence that the dealer 30 obtains the authentication of the product. The dealer 30 shows to the consumer 50 evidence that the dealer obtains the authentication of the product. Not only at the time of purchase of a brand-new product but also at the time of transaction of a second-hand product, the
20 consumer 50 can request any dealer 30 to authenticate the product and can request showing of evidence that the dealer obtains the authentication of the product.

Next, a configuration of hardware which implements the above-described embodiment of the product authentication system
25 according to the present invention is described with reference to

Fig. 2.

The ASP entity 10 who provides the product authentication service administers a database 13, a data server 14, and an authentication server 15 for passing data on the Internet.

5 The manufacturer 20, the dealer 30, and the distributor 40, who are the users of the product authentication service, keep the readers 12 leased from the ASP entity 10, and have general-purpose terminals 21, 31, and 41, such as personal computers, respectively, for connecting the readers 12 to the Internet.

10 The ASP entity 10 supplies the manufacturer 20 with the non-contact tag 11. The manufacturer 20 ships a product with the non-contact tag 11 embedded therein to the dealer 30 or to the distributor 40.

The dealer 30 and the distributor 40 deal with the product at
15 a distribution stage, and the dealer 30 ultimately sells the product to the consumer 50.

Next, information processing performed by the hardware to implement the embodiment of the product authentication system according to the present invention is described in detail with
20 reference to Fig. 3.

First, registration and browse of the product information by the manufacturer 20 are performed in the following steps.

The manufacturer 20 creates a data file based on the product information such as the name, the date of manufacture, and the place
25 of manufacture of the product manufactured with the non-contact tag

11 embedded therein. The manufacturer 20 connects the reader 12 to the Internet via the terminal 21. The reader 12 sends its own ID data to the authentication server 15. The authentication server 15 checks the received ID data of the reader 12 against the data
5 file of the reader 12 stored in the database 13. If the check tells that they are identical, the authentication server 15 automatically notifies the terminal 21 of the manufacturer 20 that the reader 12 is authenticated.

Further, if a password is assigned, the authentication server
10 15 requests the password, checks the inputted password data against the data file of the database 13. If the check tells that the they are identical, the authentication server makes a notification that the user is authenticated.

Then, the manufacturer 20 requests the data server 14 to register
15 the product information, and sends the data file of the product information, the product information being related to the ID of the non-contact tag 11. The data server 14 relates the received data file of the product information to the data file of the non-contact tag 11 which is registered in advance to update the data file of
20 the non-contact tag 11, and stores the data file in the database 13.

After the reader 12 is authenticated and the password is authenticated, the manufacturer 20 requests the data server 14 to permit browse of the product information. The data server 14 reads
25 from the database 13 the data file of the non-contact tag 11, and

sends the product information data to the manufacturer's terminal 21. The manufacturer 20 browses the product information on the manufacturer's terminal 21.

Next, the obtainment of the authentication of the product by the dealer 30 and by the distributor 40 are performed in the following steps.

First, the dealer 30 and the distributor 40 connect the readers 12 to the Internet via the terminals 31 and 41, respectively. The readers 12 send their own ID data to the authentication server 15. The authentication server 15 checks the received ID data of the readers 12 against the data files of the readers 12 stored in the database 13. If the check tells that they are identical, the authentication server 15 automatically notifies the terminals 31 and 41 of the dealer 30 and the distributor 40, respectively, that the readers 12 are authenticated.

Further, if passwords are assigned, the authentication server 15 requests the passwords, checks the inputted password data against the data files of the database 13. If the check tells that they are identical, the authentication server makes a notification that the users are authenticated.

Then, the dealer 30 and the distributor 40 read with the readers 12 the ID of the non-contact tag 11 embedded in the product for the purpose of making sure that the received product is a genuine product. Then, the authentication server 15 automatically reads the ID of the non-contact tag 11, and checks the ID against the data file of

the non-contact tag 11 stored in the database 13. Here, the authentication server 15 may also discriminate whether the product is a counterfeit or not by ascertaining whether the ID of the non-contact tag 11 relates to the manufacturer 20 who is the supplier.

5 If the check tells that they relate to each other, the authentication server 15 automatically notifies the terminals 31 and 41 of the dealer 30 and the distributor 40, respectively, that the non-contact tag 11 is authenticated, and at the same time, discloses thereto a part of the product information such as the model of the product

10 administered as the attribute information. The dealer 30 and the distributor 40 checks the disclosed product information such as the model of the product against the authenticated product to ascertain that the product is a genuine product.

A case where an attempt is made to use the product authentication system without proper authorization is now described with reference

15 to Fig. 4.

First, a case is described where the product authentication system is used with authorization. The reader 12 leased from the ASP entity 10 of the dealer 30 authorized under contract with the

20 ASP entity 10 to obtain the product authentication service can, with the specific ID of the reader 12, automatically obtain authentication of the reader 12. Further, when a password is assigned to the dealer 30 by the ASP entity 10, by checking the password, authentication of the user can be obtained. A genuine product of the dealer 30

25 can be automatically authenticated by reading with the reader the

ID of the non-contact tag 11 embedded in the product. If the product is a counterfeit, since the non-contact tag 11 is not embedded thereto, the product is not authenticated, and thus, a counterfeit can be automatically discriminated.

5 Next, a case is described where an unauthorized user steals the reader 12 leased to an authorized user from the ASP entity 10 and attempts to use the product authentication system without proper authorization. The unauthorized user can automatically obtain authentication of the reader 12. However, when the ASP entity 10
10 requires a password, since the unauthorized user does not know the password assigned to the authorized user, the unauthorized user can not input the correct password, and thus, can not obtain authentication of the user. Therefore, an unauthorized user can not obtain the product authentication service.

15 Further, a case is described where an unauthorized user counterfeits a reader and attempts to use the product authentication system without proper authorization. Even if the unauthorized user connects the counterfeit reader to the Internet, the reader can not be authenticated by the ASP entity 10. Therefore, an unauthorized
20 user can not obtain the product authentication service.

As described in the above, an object of the present invention is to provide a criterion for discrimination between genuine products and counterfeits other than the conventional outer appearance, and to make discriminating work rely not on the conventional visual and
25 manual inspection but on mechanical electronic information

processing work. By constructing on the Internet a product authentication system which solves the above object and providing the system in an ASP system as a product authentication service on the Internet to manufacturers, dealers, and distributors forming
5 a distribution channel of the products, accurate discrimination between genuine products and counterfeits in large quantity can be realized at each distribution stage from shipment from a factory of a manufacturer to arrival at a retail store at a low cost, without difficulty, at an arbitrary place, and in a short time.

10 Further, in the above product authentication system, by making a reader have its specific ID and assigning a specific password to a user for administration, unauthorized use of the product authentication system with a stolen or counterfeited reader can be prevented.

15 Therefore, counterfeits on the market can be prevented from entering the distribution channel, and benefits can be protected of all the users of the product authentication system from manufacturers manufacturing products, through dealers and distributors dealing the products, and to consumers purchasing the
20 products who are concerned with the products and who form the distribution channel.

While the description above provides a full and complete disclosure of the preferred embodiments of the present invention, various modifications, alternate constructions and equivalents may
25 be employed without departing from the true scope and spirit of the

invention.